CLAIMS

What is claimed is:

1. A digital certificate issuing system with intrusion tolerance ability, comprising:

at least one online task distributor, k online secret share calculators, m online secret share combiners and an offline secret key distributor; wherein said online task distributor is connected to said k secret share calculators through a first broadcast channel, said k secret share calculators are connected to said m secret share combiners through a second broadcast channel, said offline secret key distributor is connected to said k secret share calculators and m secret share combiners during system initialization or configuration process; wherein k and m are positive integers.

2. The system of Claim 1, further comprising an independent output interface device connected to m secret share combiners through a third broadcast channel.

3. The system of Claim 1, wherein an output interface device that is connected to said m secret share combiners through the first broadcast channel is set in said online task distributor.

4. The system of Claim 1, wherein all of at least one online task distributor, k online secret share calculators, m online secret share combiners and the offline secret key distributor are general-purpose computers or servers.

5. The system of Claim 2, wherein all of at least one online task distributor, k online secret share calculators, m online secret share combiners and the offline secret key distributor are general-purpose computers or servers.

6. The system of Claim 3, wherein all of at least one online task distributor, k online secret share calculators, m online secret share combiners and the offline secret key distributor are general-purpose computers or servers.

7. The system of Claim 1, wherein the first broadcast channel and the second broadcast channel are channels connected physically or independent channels not connected at all.

8. A digital certificate issuing method with intrusion tolerance ability, comprising the steps of distributing private key for signature of a Certificate Authority (CA) and computing digital signature for a certificate;

said distributing private key for signature of a CA comprising:

A. setting a digital certificate issuing mechanism which comprises an online task distributor, k online secret share calculators, m online secret share combiners, broadcast channels and an offline secret key distributor, wherein k and m are positive integers;

B. said offline secret key distributor expressing the private key d as a sum of t first sub-secret-keys dji and a second sub-secret-key ca; wherein d, t, c, j, i and a all are positive integers, $t < k$, j is the machine number of the jth secret share calculator, i is the secret key number inside the secret share calculators, $j = 1, 2 \ldots k$, and $i = 1, 2 \ldots l$;

C. said offline secret key distributor generating $k \times l$ random numbers as the first sub-secret-keys dji and distributing them to k secret share calculators so that each secret share calculator stores l first sub-secret-keys dji; based on the additive relation between t first sub-secret-keys and one second sub-secret- key in Step B, obtaining a group of second sub-secret-keys ca and their equation combination representations by subtracting; and then obtaining their equivalent combination sets from the equation combination representations and putting them into a large group;

D. according to combiner security condition, said offline secret key distributor searching for all equivalent combination sets in said large group and taking one combination from each equivalent combination set as a representative; putting all

representatives of equivalent combination sets into m subgroups, obtaining the second sub-secret-keys ca and their equation combination representations of the m subgroups;

E. said offline secret key distributor sending second sub-secret-keys ca and their equation combination representations of the m subgroups to m secret share combiners for pre-storage;

said computing digital signature for a certificate comprising:

F. said online task distributor sending said certificate to be signed and its hash value M to said k secret share calculators via the first broadcast channel through broadcasting data packets;

G. t or more than t secret share calculators among k secret share calculators checking correctness of said certificate to be signed based on the received certificate and its hash value M, and then making ascending power computation $M^{d_{ji}}$; sending secret share calculators number j, said processed certificate and its hash value M, the secret key number i inside the machine and I computation results $M^{d_{ji}}$ to m secret share combiners via the second broadcast channel through broadcasting data packets;

H. said m secret share combiners checking the received results, and then comparing the received results with pre-stored equivalent combination representations of the second sub-secret-keys ca and finding out a matching equivalent combination representation and the corresponding second sub-secret-key ca, and then checking correctness of said certificate to be signed; after that, multiplying ascending power computation results of t secret share calculators matching to the combination to

obtain R; finally, computing M^{c_a} based on the found ca, and multiplying M^{c_a} with R to obtain a digital signature S=Md;

l. generating a certificate based on said digital signature and the content of said certificate to be signed.

9. The method of Claim 8, Step A further comprising: setting an arbitrary number to said online task distributor, setting different numbers to k secret share calculators respectively, setting different numbers to m secret share combiners respectively and setting an initial value for t.

10. The method of Claim 8, Step C further comprising:

c1. said offline secret key distributor generating k×l random numbers as first sub-secret-keys dji and sending them to k secret share calculators with a mode accepted by administration;

c2. said offline secret key distributor solving all machine combinations from combination formula C_k^t, extending each machine combination to solve its equivalent combination set; wherein each equivalent combination set has lt combinations and each combination has t items consisted of two digits j i; and

c3. putting all equivalent combination sets into a big group.

11. The method of Claim 8, wherein said offline secret key distributor sends second sub-secret-keys c_a and their equation combination representations of the m subgroups to m secret share combiners with a mode accepted by administration in Step E.

12. The method of Claim 8, wherein said offline secret key distributor is in a physical isolation state or a shut down state after the process of distributing private key for signature of a CA has been completed through Steps A, B, C, D and E.

13. The method of Claim 8, Step F further comprising:

f1. said online task distributor receiving a digital signature task and performing a security examination and check;

f2. said online task distributor defining a task number that is unique for said task in a preset duration;

f3. said online task distributor broadcasting the online task distributor number, the task number, said certificate to be signed and its hash value M to the first broadcast channel through broadcasting data packets;

said Step G further comprising:

g1. t or more than t secret share calculators sending an acknowledgement to said online task distributor after having received said broadcasting data packets;

g2. said t or more than t secret share calculators checking uniqueness of said task; if it is determined as a new task, computing the hash value of said certificate to be signed and comparing it with a stored hash value M, if they are matched, said secret share calculators displaying said certificate to be signed, and making a ascending power computation after the displaying certificate has been confirmed by an operator; if they are unmatched or the displaying certificate is not confirmed by an operator, stopping said ascending power computation and its successive steps;

g3. said t or more than t secret share calculators broadcasting the online task distributor number, the task number and the secret share calculators number j with said task, said certificate to be signed and its hash value M, I secret key numbers and corresponding I computation results $M^{d_{ji}}$ to the second broadcast channel through broadcasting data packets;

said Step H further comprising:

h1. the secret share combiners which have received the data packets putting data packets with the same task distributor number and the same task number into a group;

h2. said secret share combiners finding out at least t data packets, and from them finding out an equation combination representation that is matched with said pre-stored equation combination representation, and obtaining corresponding second sub-secret-keys ca;

h3. computing the hash value of said certificate to be signed and comparing it with the pre-stored hash value M, if they are matched, said secret share combiners displaying said certificate to be signed and making digital signature computation after the displaying certificate is confirmed by an operator; if they are unmatched or the displaying certificate is not confirmed by an operator, stopping successive digital signature computing.

14. The method of Claim 8, wherein the processing of computing digital signature is completed through sequentially performing Steps F, G and H.

15. The method of Claim 13, wherein the processing of computing digital signature is completed through sequentially performing Steps F, G and H.

16. The method of Claim 8, further comprising Step J after Step I, said Step J comprising:

said online secret share combiners sending the digital certificate, the task distributor number and the task number to an online output interface device through broadcasting data packets; and then said output interface device verifying the digital certificate with the public key; if the digital certificate is correct, ending the digital certificate issuing task; if the digital certificate is incorrect, implementing a warning processing or an error processing.

17. The method of Claim 16, wherein online secret share combiners send the broadcasting data packets to an independent online output interface device through the third broadcast channel in Step J.

18. The method of Claim 16, wherein online secret share combiners send the broadcasting data packets to an online output interface device which is set in the task distributor through the first broadcast channel in Step J.